The Claims:

1. (Currently Amended) ~~In a network including at least one electronic device, a method of authentication of a web service customer,~~ A method comprising:

~~a web server receiving a request for access to a first web service;~~

~~intercepting the request with an agent and collecting authentication credentials;~~

intercepting at an agent a first request to grant a web service customer access to a first web service, the agent residing between the web service customer and the first web service and between the web service customer and a second web service;

collecting at the agent one or more authentication credentials of the web service customer;

determining at the agent whether the web service customer is authenticated and authorized;

if the web service customer is authenticated and authorized, ~~creating~~ at the agent:

granting the first request;

initiating creation of a session ~~and session ticket~~ and a session ticket;

~~returning an~~ obtaining a session ticket ID ~~and~~ for the session ticket ~~to the web server~~; and

encrypting the session ticket ID and a public key into an assertion;

intercepting at the agent a second request to grant the web service customer access to the second web service, the second request comprising the assertion and a private key; and

if the private key matches the public key in the assertion, granting at the agent the second request without reauthenticating or reauthorizing the web service customer.

~~sending the assertion to the first web service; and~~

~~returning the assertion to the web service customer.~~

2. (Canceled)

3. (Currently Amended) The method of claim 1, wherein the ~~request~~ assertion comprises a Security Assertions Markup Language (SAML) assertion.

4. (Canceled)

5. (Currently Amended) The method of claim 1, wherein ~~intercepting the request~~ the agent comprises an Extensible Markup Language (XML) agent ~~intercepting the request and gathering authentication credentials~~.

6. (Original) The method of claim 1, wherein determining whether the web service customer is authenticated and authorized comprises comparing the web service customer with a database containing authentication and authorization data.

7. (Currently Amended) ~~In a network including at least one electronic device, a method of authentication of a web service customer,~~ A method comprising:

~~the web service customer inserting an assertion and a signature into a document;~~

~~a webserver receiving a request for access to a web service;~~

intercepting at an agent a request to grant a web service customer access to a first web service, the agent residing between the web service customer and the first web service and between the web service customer and a second web service, the request comprising an encrypted assertion and a private key, the encrypted assertion comprising a session ticket ID for a session ticket obtained prior to the request and in response to authentication and authorization of the web service customer for access to the second web service ~~the request with an agent and collecting authentication credentials~~; and

if the private key matches the public key in the assertion, granting at the agent the second request without reauthenticating or reauthorizing the web service customer.

~~determining whether the assertion is valid;~~

~~if the assertion is valid, determining whether the web service customer is authenticated; and~~

~~if the web service customer is authenticated, granting the web service customer access to the web service.~~

8. (Currently Amended) The method of claim 7, wherein the ~~request~~ assertion comprises a Security Assertions Markup Language (SAML) assertion.

9-17 (Canceled)

18. (Withdrawn) In a network including at least one electronic device, a method of authentication of a source of a document, comprising:

a third party receiving a document from a previously authenticated first source;

the third party forwarding the document to a predetermined authentication system responsible for previously authenticating the first source to authenticate the source; and

the third party receiving an indication of validation as to whether the document originated with the first source.

19. (Withdrawn) The method of claim 18, wherein the request comprises a SAML assertion.

20. (Withdrawn) The method of claim 18, wherein receiving a document comprises a web server receiving a public key and a request for access to a web service.

21. (Withdrawn) The method of claim 18, wherein receiving a document comprises receiving an XML document without a public key.

22. (Withdrawn) The method of claim 18, wherein the predetermined authentication system comprises an XML agent intercepting the request and gathering authentication credentials.

23. (Withdrawn) The method of claim 22, wherein determining whether the document originated with the first source comprises comparing the first source with a database containing authentication and authorization data.

24. (New) The method of claim 1:

wherein the first request and the second request both originate at the web service customer; and

the method further comprising communicating the assertion to the web service customer to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

25. (New) The method of claim 1:

wherein the first request originates at the web service customer and the second request originates at the first web service; and

the method further comprising communicating the assertion to the first web service to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

26. (New) An apparatus comprising:

one or more processors residing between the web service customer and the first web service and between the web service customer and the second web service; and

a memory coupled to the processors comprising one or more instructions executable at the processors, the processors operable when executing the instructions to:

intercept a first request to grant a web service customer access to a first web service;

collect one or more authentication credentials of the web service customer;

determine whether the web service customer is authenticated and authorized;

if the web service customer is authenticated and authorized:

grant the first request;

initiate creation of a session and a session ticket;

obtain a session ticket ID for the session ticket ; and

encrypt the session ticket ID and a public key into an assertion;

intercept a second request to grant the web service customer access to the second web service, the second request comprising the assertion and a private key; and

if the private key matches the public key in the assertion, grant the second request without reauthenticating or reauthorizing the web service customer.

27. (New) The apparatus of claim 26, wherein the assertion comprises a Security Assertions Markup Language (SAML) assertion.

28. (New) The apparatus of claim 26, wherein the agent comprises an Extensible Markup Language (XML) agent.

29. (New) The apparatus of claim 26, wherein the processors are further operable when executing the instructions to determine whether the web service customer is authenticated and authorized by comparing the web service customer with a database containing authentication and authorization data.

30. (New) The apparatus of claim 26, wherein:

the first request and the second request both originate at the web service customer; and

the processors are further operable when executing the instructions to communicating the assertion to the web service customer to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

31. (New) The apparatus of claim 26, wherein:

the first request originates at the web service customer and the second request originates at the first web service; and

the processors are further operable when executing the instructions to communicate the assertion to the first web service to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

32. (New) A system comprising:

a first web service;

a second web service; and

an agent residing between a web service customer and the first web service and between the web service customer and the second web service, the agent operable to:

intercept a first request to grant the web service customer access to the first web service;

collect one or more authentication credentials of the web service customer;

determine whether the web service customer is authenticated and authorized, and if the web service customer is authenticated and authorized:

grant the first request;

initiate creation of a session and a session ticket;

obtain a session ticket ID for the session ticket; and

encrypt the session ticket ID and a public key into an assertion;

intercept a second request to grant the web service customer access to the second web service, the second request comprising the assertion and a private key; and

if the private key matches the public key in the assertion, grant the second request without reauthenticating or reauthorizing the web service customer.